附件3

山西省通信管理局

网络安全威胁处置通知书

网安处字〔202 〕 号

：

工业和信息化部/我局委托

于202 年 月 日监测发现，你单位

网站/系统存在网页篡改/植入暗链/植入后门/ 漏洞/

（详见附件）。

依据《网络安全法》《互联网信息服务管理办法》（国务院令第292号）及工业和信息化部《公共互联网网络安全威胁监测与处置办法》相关规定，我局已暂停该网站/系统接入/ ，请自收到本通知书 个工作日内整改漏洞/清除恶意程序，并对本单位其他网站/系统进行检查，处置类似网络安全威胁，消除安全隐患/影响。处置情况于处置后 个工作日内回复我局，并提供最近一次的网站/系统风险评估报告（具备资质的第三方出具）。我局将视情况进行验证。拒不处置的，我局将依法实施行政处罚。

附件：网络安全威胁事件情况通报（模板1－5）

山西省通信管理局（公章）

年 月 日

我局地址：山西省太原市南内环街2号 邮编：030006

联系人： 联系电话：

邮箱：

抄送：

模板1：

“xx网”网站被恶意篡改

1.网络安全事件名称：“xx网”网站被恶意篡改

2.网站名称：

3.网站域名：

4.网站IP地址：

5.网站漏洞URL：http://

6.事件类型：网页篡改

7.危害描述及证明：

8.处置建议：

（1）首先将网站进行下线处理，然后删除被篡改的页面，恢复至原有的页面；

（2）对网站系统做网络安全风险评估，并对其漏洞进行修复；

（3）修改网站后台、服务器管理员和数据库相关口令。

模板2：

“xx网”网站被植入黑链

1.网络安全事件名称：“xx网”网站被植入黑链

2.网站名称：

3.网站域名：

4.网站IP地址：

5.网站漏洞URL：http://

6.事件类型：网页黑链（单击鼠标右键查看源代码即可找到被植入的黑链）

7.危害描述及证明：

8.处置建议：

（1）清理网站页面内的黑链代码，通常黑链代码的标签都是成对出现的，将黑链标签内的代码删除；

（2）对网站系统做网络安全风险评估，并对其漏洞进行修复；

（3）修改网站后台、服务器管理员和数据库相关口令。模板3：

“xx网”网站被植入后门程序

1.网络安全事件名称：“xx网”网站被植入后门程序

2.网站名称：

3.网站域名：

4.网站IP地址：

5.网站漏洞URL：http://

6.事件类型：网站后门

7.危害描述及证明：

8.处置建议：

（1）排查并清除掉潜在的网页后门，并进行全盘病毒查杀;

（2）对网站系统做网络安全风险评估，并对其漏洞进行修复；

（3）修改网站后台、服务器管理员和数据库相关口令。

模板4：

“xx网”网站存在xx漏洞

1.网络安全事件名称：“xx网”网站存在xx漏洞

2.网站名称：

3.网站域名：

4.网站IP地址：

5.网站漏洞URL：http://

6.事件类型：网站漏洞

7.危害描述及证明：

8.处置建议：

（1）升级系统版本，针对该漏洞打漏洞补丁;

（2）向厂家申请提供漏洞修补方案；

（3）其他针对性建议视具体情况填写。

模板5：

xx系统存在xx漏洞

一、xx漏洞

1.漏洞名称

2.漏洞类型

3.风险程度

4.漏洞描述及证明

5.漏洞修复建议

二、xx漏洞

1.漏洞名称

2.漏洞类型

3.风险程度

4.漏洞描述及证明

5.漏洞修复建议